



Appointing a
Data Protection Officer

INTRODUCTION

In this, the forth of a series of linked articles about **Data Protection Officers** (DPOs) under the **General Data Protection Regulation** (GDPR), we examine some important aspects related to the appointment of a DPO.

Once it has been established that a **DPO is required** and the **role of the DPO** is confirmed, careful consideration must be given to making the right selection. This process is not only about identifying the correct individual (or specialist provider) but also ensuring the position is correctly appointed and in the best interests of the organisation as a whole.

CONTENTS

Page **3**

Key facts about appointing a DPO

Page **4**

The GDPRs provisions for appointing a DPO

Page **5**

The WP29 guidelines on DPOs comments on appointing a DPO

Page **10**

Internal of external appointment

Page **13**

Internal DPO

Page **14**

External DPO

Page **15**

Register your DPO with the ICO

Page **16**

DPO Resources

Page **21**

Practical steps for appointing a DPO

Page **24**

Dismissing a DPO

Page **25**

Final words

Page **26**

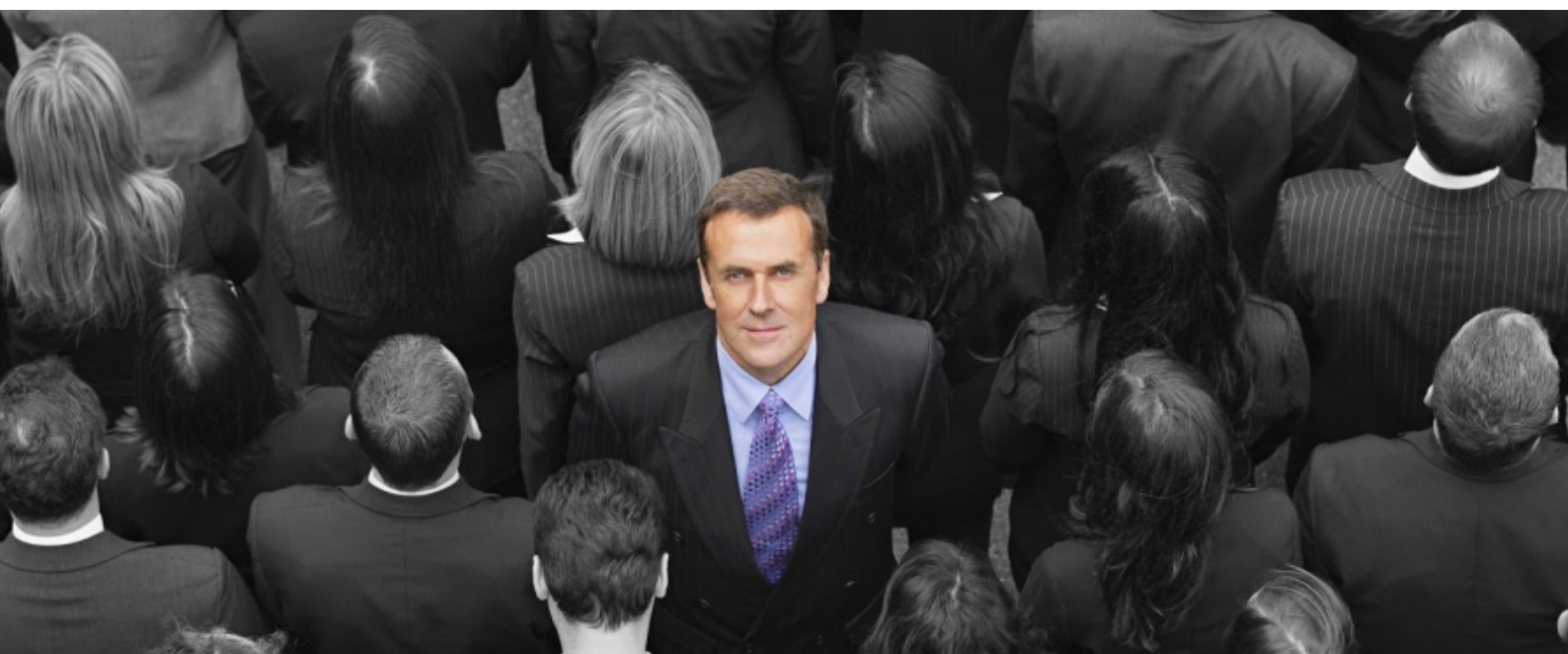
Available Courses

KEY FACTS ABOUT APPOINTING A DPO

- The appointment of a DPO can help facilitate GDPR compliance. It is important to note, however, that the DPO is not personally liable in case of a breach of data protection law, and that responsibility for compliance remains with the employer.
- The DPO can be an internal staff member or an external consultant. The size and scope of the data processing operations may result in a part-time appointment for smaller organisations, whereas a DPO team may be necessary for larger organisations. The same DPO can even represent multiple organisations but must be accessible by the customers, service users, and employees of each establishment.
- Ideally, the DPO should be located within the European Union and must be in a position to communicate in the language of the data subjects and the supervisory authority.
- Give careful consideration to the ethical nature of the role and rule out any conflict of issues before making an appointment. Once in position, the DPO becomes responsible for all the processing activities carried out by the organisation.
- Ensure that the DPO is a suitably qualified and senior appointment, supported with the necessary resources to lead data protection compliance. To allocate those resources effectively, the selected DPO will need a background in project management and be able to demonstrate effective leadership skills. The DPO must also be able to evaluate themselves for knowledge gaps and request training in those areas.
- The DPO should have experience in dealing with different cultures and methods of doing business. Think of a retailer operating in the UK, who manufacturers in China, outsources in India, and has its headquarters in the US. The DPO will require the versatility to lead and direct data processing operations across multiple territories (with overlapping data privacy and cybersecurity regulations) in order to achieve a successful outcome.
- The DPO should be a confident, self-motivated and competent professional who can carry out their responsibilities without guidance or interference. They require a presence at board-level and will need to be able to deal with accomplished business professionals who may not know the complexities of data protection law.

THE GDPR PROVISIONS FOR APPOINTING A DPO

Article 37 outlines the requirements for appointing a DPO. It states how the position must be filled by someone who has an in-depth knowledge of data protection law and can fulfil the tasks set out in **Article 39**. It goes on to state that the role of the DPO may be an internal position or fulfilled by an external service provider. And that a group of enterprises may appoint a single DPO so long as they are equally accessible to all establishments. Finally, if either the controller or the processor is a public authority or body, then a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size.



THE WP29 GUIDELINES ON DPOS COMMENTS ON APPOINTING A DPO

The Article 29 Working Party (WP29) [Guidelines for Data Protection Officers](#)¹ provide a wealth of information regarding how to interpret GDPR provisions, including:

- The professional qualities of a DPO
- The conditions in which organisations can jointly appoint a DPO
- Where a DPO should be located
- The resources a DPO should be provided with

These will be examined in detail throughout the rest of this document.

PROFESSIONAL QUALITIES OF A DPO

Article 37(5) of the GDPR states:

The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39.

The WP29 Guidelines provides:

The necessary level of expert knowledge should be determined according to the data processing operations carried out and the protection required for the personal data being processed. For example, where a data processing activity is particularly complex, or where a large amount of sensitive data is involved, the DPO may need a higher level of expertise and support.

Relevant skills and expertise include:

- Expertise in national and European data protection laws and practices including an in-depth understanding of the GDPR
- Understanding of the processing operations carried out
- Understanding of information technologies and data security
- Knowledge of the business sector and the organisation
- Ability to promote a data protection culture within the organisation

THE WP29 GUIDELINES ON DPOS

COMMENTS ON APPOINTING A DPO CONT.

The Information Commissioners Office (ICO) offers [similar guidance](#), stating that although the GDPR does not stipulate the exact qualities a DPO must have, the person or external specialist appointed must have the credentials required, which are:

Proportionate to the type of processing you carry out, taking into consideration the level of protection the personal data requires.

In addition, the ICO states that,

Although not mandatory, it is an advantage for a DPO to have a strong knowledge of the industry or sector they are operating in.

In the article [The Role of the DPO – What you need to know](#), authors Anita Bapat and James Henderson discuss that is currently not clear what level of knowledge a DPO will be required to hold. They go on to predict that uniform standards are likely to develop as time goes on.

“

We would expect common standards to be developed in due course, possibly including EU-wide certification programs for individuals to demonstrate they have the appropriate knowledge of data protection law to perform the role of DPO

[Anita Bapat & James Henderson, Hunton & Williams](#)

Back in 2013, Lisa Jackson, Solicitor and Data Protection Practitioner with Leman Solicitors in Ireland² states that the position of DPO would lend itself well to someone with a legal or compliance background.

However, whilst knowledge of data protection law is clearly essential, a DPO, especially in a large organisation, may struggle to perform their duties without a background in IT.

Take the case of a personal data breach, [Article 33\(1\)](#) of the GDPR directs that:

THE WP29 GUIDELINES ON DPOS

COMMENTS ON APPOINTING A DPO CONT.

The controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with [Article 55](#), unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

Furthermore, under [Article 34\(1\)](#):

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

Given the fact that one of the DPOs key tasks under Article 39(2) is:

The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

As you can see, it would be hard to imagine how a DPO could provide the controller with the information required to meet breach disclosure deadlines without a competent knowledge of IT systems, data mapping, and the skills to locate the source of a data breach.

Although the task of locating the breach and identifying data subjects affected are likely to be performed by the IT department, the DPO must have a rudimentary understanding of the concepts in order to communicate effectively to the controller or processor, the ICO, all the affected data subjects, and any other stakeholders.

The same applies to carrying out effective Data Protection Impact Assessments (DPIA).

SOFT SKILLS ARE OF EQUAL IMPORTANCE

In addition to legal, compliance, and IT skills and knowledge, a DPO must also have strong business acumen. Organisations should look to hire DPOs who have solid business sense, along with good management and communication skills, not just legal know-how.

In his article, [Companies Need Data Protection Officers With Business Acumen](#), George Lynch quotes Bojana Bellamy, president of the Centre for Information Policy Leadership in London, who states unequivocally that:

THE WP29 GUIDELINES ON DPOS COMMENTS ON APPOINTING A DPO CONT.

“

Business skills are critical to be a successful DPO.

Bojana Bellamy, Centre for Information Policy Leadership

Lynch goes on to quote Winston Maxwell, privacy partner at Hogan Lovells LLP in Paris who comments that DPOs with a strict legal background are likely to focus on the risks a proposed processing activity might create, rather than look at the bigger picture and provide management with opportunities and solutions to allow them to move forward.

“

The DPO needs to be a facilitator and communicator as they need the ability to bring everyone in the organisation together to focus on privacy and data security.

Winston Maxwell, Hogan Lovells LLP

These vital communication skills need to extend outside the organisation. For example, all supplier contracts in which data processing is a part need to include terms which ensure all GDPR provisions will be complied with by the external supplier.

As with overall compliance with the GDPR, responsibility for supply-chain contracts ultimately lies with the controller. However, in many (if not most) cases, the DPO will have a lead role in ensuring each contract meets compliance requirements.

It is clear therefore that a DPO must be able to negotiate contractual terms, sometimes in cross-border situations, which ensure not only that compliance is met, but also that the best interests of the DPOs employer are protected and advanced.

A DPO must be a good listener and be able to tune into the internal politics of an organisation. Joyce Allen, Founder and Principal Training Consultant at Freevacy states:

THE WP29 GUIDELINES ON DPOS COMMENTS ON APPOINTING A DPO CONT.

“

All of a sudden, different divisions of the organisation are being asked to invite this new officer into working groups, project meetings, and accept their recommendations as they plan new projects. Many of whom will never have considered taking advice about data protection in the past. You can imagine how this could become a difficult pill to swallow if the DPO has no diplomacy skills.

Joyce Allen, CIPP/E, BCS Practitioner in DPA18 & FOIA | Freevacy

Finally, a point of paramount significance, due to the nature and purpose of the role, a DPO must possess a high degree of integrity, honesty, and professional ethics in order to achieve his or her objectives satisfactorily.

INTERNAL OR EXTERNAL APPOINTMENT

One of the key questions an organisation who is obliged by law or has decided voluntarily to appoint a DPO must ask is whether it is best to appoint an internal DPO or contract out the function to an external specialist.

Article 37(6) provides that:

The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.

This makes practical sense, as, according to initial research conducted by the International Association of Privacy Professionals (IAPP) in 2016, a predicted **75,000 DPOs would be needed** around the world to manage personal data belonging to EU citizens.

However, on the first anniversary of the GDPR having taken effect, a subsequent IAPP study indicates that a staggering **half-million organisations have already registered DPOs**.

Also, when this research is combined with data from IAPP's latest **salary survey**, it sheds light onto the rapid growth of the privacy profession and the expanding role of DPOs in Europe and beyond.

“

An estimated a 500,000 organisations have registered DPOs across Europe alone.

International Association of Privacy Professionals

If the IAPP's analysis is accurate, there simply aren't anywhere near enough experienced data protection practitioners to go around. By way of confirmation, in November 2019 Jennifer A. Kingson, a former editor of the New York Times, discusses this very point in an article for Axios about **the global shortage of privacy experts**, saying:

“

It's more important than ever companies have privacy experts, to help them obey proliferating laws on how consumers' data can be used — but it's hard to find people with the expertise to do it.

Jennifer A. Kingson, Axios

INTERNAL OR EXTERNAL APPOINTMENT CONT.

Given the global shortage of experienced privacy professionals, the probability of finding a suitable candidate to fulfil the role of the DPO is less than likely. Not without paying a premium at least.

Under the circumstances, two realistic options remain:

- > Appoint an existing employee(s) and enrol them on a **certificated GDPR training course**
- > Look for an external provider or contractor with the relevant skill set

Specialist external providers will fill a gap in the market, especially for organisations that lack the financial resources to hire someone specifically for the role.

An external DPOs perspective

One such company, **Veritau Ltd**, acts as the Data Protection Officer for over 500 public sector schools and councils in the North of England. Becky Bradley, Information Governance Manager at Veritau, had this to say about the benefits of obtaining an external DPO service: "It means having easy access to a team of independent specialists. It means not having to train in-house staff to carry out the work, or employing someone solely to undertake the role. It also helps to avoid potential conflicts of interest."

When it comes to identifying the right provider Becky recommends: "look for a specialist that offers a systematic approach to developing Data Protection compliance. By providing templates, guidance, compliance audits and the training needed to fulfil their clients Data Protection obligations, it removes the need to develop these from scratch. They should have a trained team of Data Protection experts, who keep up to date with legislative and regulator developments."

“

**Always check sector experience and qualifications,
as you need the assurance that you will be supported
with the right advice when it is most needed.**

Becky Bradley, BCS Practitioner in DPA18 & FOIA | Veritau Ltd

INTERNAL OR EXTERNAL APPOINTMENT CONT.

The WP29 DPO Guidelines provide that where a specialist provider is engaged as a DPO:

A team of individuals working for that entity may effectively carry out the DPO tasks as a team, under the responsibility of a designated lead contact and **person in charge** of the client. In this case, it is essential that each member of the external organisation exercising the functions of a DPO fulfils all applicable requirements of the GDPR.

The Guidelines also state that for the purposes of clarity and to avoid conflicts of interests, where a specialist external DPO is appointed each person assigned to manage a particular client should have a set allocation of tasks. In addition, one person should be allotted as a key contact for the organisation and external stakeholders such as customers and suppliers.

There are advantages and disadvantages to both an internal and external appointment of a DPO.

INTERNAL DPO

ADVANTAGES

The position can be filled internally by a person who already has an in-depth knowledge of the organisation and industry.

Being on-site provides the DPO with access to all internal stakeholders, and it is less likely senior management will forget to consult with them on data protection matters.

The DPO will enjoy the protection of employment law and will be provided with the resources (both technical and personnel) by the controller.

DISADVANTAGES

It may be difficult to find a single person who possesses the legal, IT, and business knowledge, as well as soft skills such as negotiating and communicating excellence.

Because the DPO is a staff member, it may be more difficult for them to maintain the independence mandated by Article 38 of the GDPR.

Your organisation may require a flexible option regarding a DPO. For example, you may not require a DPO for any more than a few hours a month. If this is the case, then with the absence of having to pay holiday pay, pensions, and other employee benefits, outsourcing the role of DPO to an external provider will be more cost-effective than an internal appointment.

EXTERNAL DPO

ADVANTAGES

A specialist provider will have the spread of skills necessary to perform the tasks required of a DPO.

Flexibility in terms of cost and how many hours are required. For example, the service contract can allow for an increase in hours at the beginning of a project when Data Protection Impact Assessment (DPIA) work is at its most demanding.

An external DPO is naturally independent, and there is no pressure to provide them with extra tasks, which may pose a conflict of interest, in order to justify the investment in their position.

DISADVANTAGES

The external supplier may not have an in-depth knowledge of the organisation's industry or sector.

Because the DPO is external, there may be a disconnect between the office and the company. This raises the risk of the DPO provider not being informed and consulted on matters concerning data protection – which amounts to a compliance breach.

Many service contracts will charge on a per-hour basis. This risks becoming expensive when the time taken for attending regular meetings and training internal staff is taken into consideration.

REGISTER YOUR DPO WITH THE ICO

If you have made an appointment, **you need to register your DPO with the ICO** as soon as possible. To do this, email dataprotectionfee@ico.org.uk and put **Add a DPO** in the subject line.

You should include in the body of the email:

- Your company's registration number
- Whether you are required to appoint a DPO or are doing so voluntarily
- The name, address, phone number and/or email address of your DPO if they are an individual (eg a member of staff or a member of your organisation); or
- The name, address, phone number and/or email address of the external organisation that will be carrying out the DPO duties on your behalf

You will also need to state whether you wish to have the name of your DPO published on the data protection register.



DPO RESOURCES

Complying with the GDPR means a DPO, whether internal or external, must have access to the resources required to perform their tasks under Article 39.

WP29 Guidelines states:

The DPO must have the resources necessary to be able to carry out his or her tasks.

Depending on the nature of the processing operations and the activities and size of the organisation, the following resources should be provided to the DPO:

- Active support of the DPOs function by senior management
- Sufficient time for DPOs to fulfil their tasks
- Adequate support in terms of financial resources, infrastructure (premises, facilities, equipment) and staff where appropriate
- Official communication of the designation of the DPO to all staff
- Access to other services within the organisation so that DPOs can receive essential support, input, or information from those other services
- Continuous training

The International Association of Privacy Professionals (IAPP) provides a [toolkit for DPOs](#) (note that you must be a member to gain access). To provide an example of the investment required to fund a data protection program it illustrates the following:

How much does it cost to fund a data protection program?

Budget & Employees required



 Full Time Employee  Part Time Employee

Source: 2016 IAPP-EY Privacy Governance Report

To ensure compliance, it is imperative a DPO is properly resourced, and this should be factored into the overall DPO budget.

DPO RESOURCES CONT.

DPOS FOR MORE THAN ONE BUSINESS

A single DPO can be contracted across more than one organisation.

Article 37(2) states:

A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.

When defining the term **accessibility** the WP29 DPO Guidelines relates it to:

The tasks of the DPO as a contact point with respect to data subjects, the supervisory authority but also internally within the organisation.

This means their contact details must be available and they communicate in the language of the data subjects and supervisory authority. It is critical, therefore, that if a DPO is designated to cover multiple organisations, they are provided with the resources and team members to ensure they are always contactable by data subjects and authorities, and can comply with their performance obligations.

CONFLICTS OF INTEREST

A key concern with designating one DPO for multiple organisations is that the officer and/or their team will encounter situations where there is a conflict of interest. In fact, conflicts of interests are something that controllers and processors must constantly be alert to when selecting a DPO.

Article 38(6) makes it clear that:

The data protection officer may fulfil other tasks and duties.

However, it goes on to state that the organisation must:

Ensure that any such tasks and duties do not result in a conflict of interests.

While the GDPR does not define what constitutes a conflict, the WP29 DPO Guidelines offer the following advice to avoid conflicts:

The DPO cannot hold a position within the organisation that leads him or her to determine the purposes and the means of the processing of personal data.

DPO RESOURCES CONT.

Senior management positions, which are likely to cause conflicts include:

- Chief executive
- Chief financial officer
- Head of marketing
- Head of IT
- Head of human resources

It is important to note that it is not just senior positions that should be considered a risk. Some positions lower down the organisational hierarchy may involve determining the purposes and means of processing, which will rule them out as feasible roles for DPOs.

To avoid conflicts of interests, the DPO Guidelines suggest organisations should:

- Work out what positions are incompatible with that of a DPO
- Draw up policies and procedures based on those findings
- Explain what is meant by conflict of interest in those policies and procedures
- State that the DPO does not have any conflicts of interest
- Include safeguards in the internal rules of the organisation and ensure that the job specification for the position of DPO or the service contract is sufficiently precise and detailed to avoid conflicts of interest

In the case of an external provider, best practice recommends that the organisation documents the steps it has taken to avoid conflicts of interest and has an ongoing policy of how to deal with conflicts should they arise in the future.

THE LOCATION OF THE DPO

The WP29 DPO Guidelines are clear about where the DPO should be located:

To ensure that the DPO is accessible, the WP29 recommends that the DPO be located within the European Union.

DPO RESOURCES CONT.

This approach is considered the best-case scenario even if this is not where the organisation is located.

However, it is recognised that in situations where the organisation has no establishment in the EU, it may be more effective for the DPO to be located outside the bloc. An obvious example of this will be the UK, which has implemented the principles of the GDPR through the Data Protection Act 2018 but will be leaving the EU on the 31 October 2019. In most circumstances, having the DPO based in the UK would not pose any issues with relation to the ability to adequately perform the tasks required.







As for multi-nationals who process the data of EU subjects, the DPO Guidelines appear to recognise the commercial reality and that such organisations should be able to designate a DPO who is based elsewhere.

In some situations where the controller or the processor has no establishment within the European Union, a DPO may be able to carry out his or her activities more effectively if located outside the EU.

PRACTICAL STEPS FOR APPOINTING A DPO

Whether you are making an internal or external appointment, there are certain provisions which need to be included in the employment contract/service agreement or outsourcing agreement.









As with all contracts, your documents should be drafted/reviewed by a legal professional.

CONTRACT AREA	INTERNAL POSITION	EXTERNAL APPOINTMENT
Add the names of the parties identifying the employer or contractor as the controller plus one of the following as the DPO.	Candidate or employee.	Specialist external contractor or DPO service provider.
Outline the duties of position / services to be provided.	The duties of the position should include the tasks listed in Article 39 plus any other responsibilities associated with the DPO role or other unrelated tasks, taking care there is no conflict of interest.	The contract must include as a minimum the tasks listed in Article 39, along with any additional services specific to the organisation. Ensure that the scope is clearly defined.
List the responsibilities of the controller or processor as required under Articles 37-38, and any compliance obligations under local law.		
Identify where the role of DPO sits within the organisation.		
Confirm who the DPO reports to within the organisation, remembering that it should be at the highest management level.		

PRACTICAL STEPS FOR APPOINTING A DPO CONT.

CONTRACT AREA	INTERNAL POSITION	EXTERNAL APPOINTMENT
Clarify the controller's area of business and the market sectors in which they operate.	—	✓
Ensure the DPO has professional liability insurance to address claims for negligence in the performance of their duties.	—	✓
Add a clause indemnifying the DPO against third-party legal action, and limiting the legal liability exposure.	—	✓
Add a clear statement requiring there is no conflict of interest. Also, any future conflicts will be notified to the controller or processor as soon as they are identified and are to be addressed immediately.	✓	✓
To further limit potential conflicts of interest, it may be advisable to compensate DPOs in the form of cash payments, rather than stock options or packages tied to company performance.	Salary, bonuses, pension, holiday, medical cover etc.	Fixed contract or hourly rate. Make allowance for how the provision of additional services or hours will be requested and approved.
Define the resources provided by the controller to allow the DPO to perform their tasks.	✓	✓

PRACTICAL STEPS FOR APPOINTING A DPO CONT.

CONTRACT AREA	INTERNAL POSITION	EXTERNAL APPOINTMENT
Allow for how the DPO will maintain their skills with ongoing training and development.	Agree in advance the provisions and requirements for continuous professional development.	Add a clause requiring the DPO to maintain their competence in data protection and related areas.
Define the provisions for obtaining legal advice or other expert opinions and services.		
Outline the procedure to handle differences of opinion where the controller and the DPO do not agree upon an important issue related to GDPR compliance.		
Provide an adequate minimum contract term that will allow the DPO to assess and implement the required changes to bring about GDPR compliance.		
Add a clause stating that the DPO will uphold professional and legal requirements of confidentiality and secrecy.		
Clarify the reasons which could lead to the dismissal or early termination of the DPOs contract.	Provide redundancy and termination of employment information.	Define the circumstances in which the contract will be terminated and how personal data is returned or deleted.

DISMISSING A DPO

It is important to understand the circumstances in which the DPO is protected against unfair dismissal simply for carrying out their role.

Article 38(3) of the GDPR states:

He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks.

For example, if the DPO regards a particular data processing activity as high risk and recommends that a DPIA should be undertaken, he or she cannot be dismissed for providing such advice, even if it results in a delayed project and/or lost income.

Other forms of penalties include:

- Being held back or prevention from career advancement
- Withholding benefits that other employees receive

It is not necessary for a penalty to actually be carried out. Used to punish a DPO for carrying out their duties, a threat alone is enough to constitute improper conduct by the employer.

A DPO, however, is not protected from dismissal for conduct or actions undertaken outside the performance of the tasks defined under Article 39(1). Furthermore, protection from dismissal will not apply in other circumstances, such as the following:

- Criminal acts or gross misconduct (theft, physical, psychological or sexual abuse)
- Bankruptcy of the organisation
- Being intoxicated on drugs or alcohol whilst at work

Organisations should expect that a former DPO may seek to challenge a decision not to renew their service contract using the argument they were dismissed for performing their tasks. This could lead to a contract law dispute.

There is little doubt such a case will come before the courts at some point in the future, a move that will hopefully clarify the law in this area. Until then, organisations engaging an external provider should take care to document everything in relation to the provider's performance or lack thereof.

FINAL WORDS

Appointing a DPO requires careful consideration of a range of factors, including whether to hire someone on a temporary, part-time, or full-time basis or to outsource to a specialist provider. Thought must also be given as to the resources required by the DPO so they can perform their tasks in relation to the particular needs of **your business**, and how to avoid conflicts of interest.

When it comes to appointing a DPO, preparation is key. Abraham Lincoln said that if he had eight hours to chop down a tree, he would spend six sharpening his axe. This is still prudent advice for anyone looking at filling a DPO position within their organisation.

1. The Article 29 Working Party (WP29) was transformed into the “European Data Protection Board” (“EDPB”) under the GDPR
2. Jackson, Lisa, "The expanded role of the DPO" PDP Journals, Volume 13, Issue 5, 2013

SEE OUR AVAILABLE COURSES



BCS Foundation Certificate in Data Protection

The Foundation GDPR Certificate from the BCS is recommended for anyone involved in the collection, usage or protection of personal information.

[FIND OUT MORE](#)



IAPP Certified Information Privacy Professional Europe

The CIPP/E is the essential IAPP certification for privacy professionals covering Europe's framework of laws, regulations and policies, most significantly the GDPR.

[FIND OUT MORE](#)



BCS Practitioner Certificate in Data Protection

The GDPR Practitioner Certificate from the BCS is the leading industry qualification for UK focused DPOs and compliance professionals.

[FIND OUT MORE](#)



IAPP Certified Information Privacy Manager

The CIPM is a unique qualification in privacy programme management from the IAPP that teaches DPOs and senior compliance professionals how to turn policies into accountability.

[FIND OUT MORE](#)



BCS Practitioner Certificate in Freedom of Information

This BCS Practitioner Certificate is the recognised qualification for individuals with information access responsibilities under the FOIA or EIR.

[FIND OUT MORE](#)



IAPP Certified CIPP/E & CIPM Combination course

These two combined practitioner level certified courses from the IAPP are recommended for DPOs and other compliance professionals with privacy operations' responsibilities.

[FIND OUT MORE](#)

NEXT GUIDE IN THE SERIES

What to do when not appointing a Data Protection Officer

In this, the fifth of a series of linked articles about Data Protection Officers (DPOs) under the General Data Protection Regulation (GDPR), we discuss how an organisation can implement and maintain a privacy compliance programme when it is not required to appoint a DPO and chooses not to do so voluntarily.

[DOWNLOAD GUIDE](#)





Freevacy is an independent GDPR training provider. We offer accredited BCS and IAPP training for DPOs, privacy professionals and anyone with data protection responsibilities. We also deliver bespoke courses that can be adapted to suit your particular learning requirements.

For more information, please call: 0370 04 27001
or email: **contact@freevacy.com**

www.freevacy.com